Requested Patent: WO0135334A1

Title:

CREDIT CARD WITH FINGERPRINT AUTHENTICATION SYSTEM ;

Abstracted Patent: WO0135334 ;

Publication Date: 2001-05-17 ;

Inventor(s): LI KENNETH (US) ;

Applicant(s): LI KENNETH (US) ;

Application Number: WO2000US31425 20001113 ;

Priority Number(s): US19990164969P 19991111 ;

IPC Classification: G06K19/06; G06K5/00 ;

Equivalents: AU1767201 ;

ABSTRACT:

A credit card (10) having a processor (36), a memory (32) connected to the processor (36) that stores credit card identification information for at least one credit account, a scanner (34) connected to the processor (36), and a transmitter (12) connected to the processor (36); the processor (36) is programmed to receive reference fingerprint data from the scanner (34), store reference data based on the reference fingerprint data into the memory (32), receive test fingerprint data from the scanner (34) at a time after the reference data is stored in memory (32), compare the reference data with test data based on the test fingerprint data and only if the comparison is within predefined limits, send the credit card identification information to the transmitter (12).

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 May 2001 (17.05.2001)

PCT

(10) International Publication Number
WO 01/35334 A1

(51) International Patent Classification[7]: G06K 19/06, 5/00

(21) International Application Number: PCT/US00/31425

(22) International Filing Date:
13 November 2000 (13.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/164,969 11 November 1999 (11.11.1999) US

(71) Applicant and
(72) Inventor: LI, Kenneth [US/US]; 217 Laurel Avenue, Arcadia, CA 91006 (US).

(74) Agent: MONROE, Wesley, W.; Christie, Parker & Hale, LLP, 350 West Colorado Boulevard, P.O. Box 7068, Pasadena, CA 91109-7068 (US).

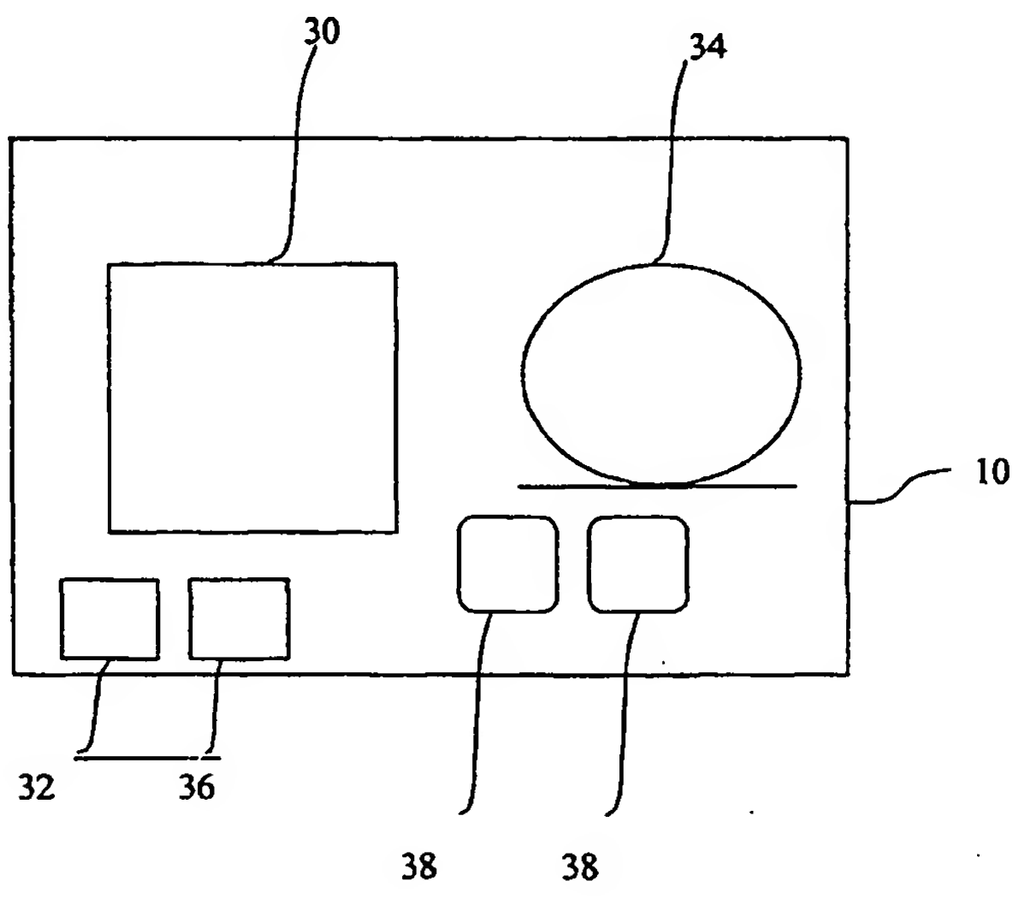
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: CREDIT CARD WITH FINGERPRINT AUTHENTICATION SYSTEM



(57) Abstract: A credit card (10) having a processor (36), a memory (32) connected to the processor (36) that stores credit card identification information for at least one credit account, a scanner (34) connected to the processor (36), and a transmitter (12) connected to the processor (36); the processor (36) is programmed to receive reference fingerprint data from the scanner (34), store reference data based on the reference fingerprint data into the memory (32), receive test fingerprint data from the scanner (34) at a time after the reference data is stored in memory (32), compare the reference data with test data based on the test fingerprint data and only if the comparison is within predefined limits, send the credit card identification information to the transmitter (12).

WO 01/35334 A1

1

CREDIT CARD WITH FINGERPRINT AUTHENTICATION SYSTEM

BACKGROUND OF THE INVENTION

Most credit card authorization systems consist of a scanner which electronically scans a magnetic strip on a credit card using a mechanically contacting magnetic head. An example of a credit card with a magnetic strip is shown in FIG. 1. With repeated use, the mechanical contact often fails. Therefore, it is desirable to have a credit card that is electronic and has a non-contact means of transmitting information. Thus, it has been the goal of many applications to change from the current system to a non-contact system. A system for non-contact data transfer was disclosed by Kenneth Li, disclosure document No. 401597, the entire contents of which are incorporated herein by reference.

Common methods of non-contact information transfer are found in remote controls of TV's and VCR's, etc. Common methods employ infra-red light, induction, or radio frequency. However, the common methods discussed above tend to consume a lot of power and therefore, are not suitable for a credit card with a small size.

Further, the current system of using a credit card with a magnetic strip for electronic transfer of funds or point of sale transactions is subject to fraud. Thus, there is a need for security so that stolen or misplaced cards are not used by people other than the owner.

SUMMARY OF THE INVENTION

The present invention overcomes the problems of the prior art by using a passive optical shutter to provide an optical signal for a card reader. The optical shutter may be a liquid crystal shutter. The controlling of a liquid crystal shutter requires very little power thus allowing for information transfer using a small amount of power, and for an increased range of

applications. Additionally, the present invention provides a fingerprint authentication system.

In one embodiment a credit card is manufactured with a processor. A memory for storing credit card identification information for at least one credit account is connected to the processor. A scanner and a transmitter are also connected to the processor. The transmitter may be a transmissive shutter, a reflective shutter, an induction coil, an infrared transmitter, a radio transmitter and smart card electrical contacts.

The processor is programmed to receive reference fingerprint data from the scanner and to store reference data based on the reference fingerprint data into the memory. The processor receives test fingerprint data from the scanner at a time after the reference data is stored in memory, and compares the reference data with test data based on the test fingerprint data. The processor sends the credit card identification information to the transmitter only if the comparison is within predefined limits.

In an embodiment of the present invention, the reference data is an identification code derived from the reference fingerprint data and the test data is a test code derived from the test fingerprint data. In an alternative embodiment, the reference data is derived from the reference fingerprint data using one of several algorithms. An identifier of the selected algorithm is stored in the memory. Test data is obtained from the test fingerprint data based on the identification of the selected algorithm. In another alternative embodiment, the reference data is a subset of the reference fingerprint data and the test data is a subset of the test fingerprint data.

The card may also have a solar cell for power connected to the processor, memory and scanner. Additionally, the card may have a receiver for receiving information from an external machine or another card.

In one embodiment of the present invention, the memory only accepts reference data once. The memory may be configured to store identification information for more than one credit account. If the memory is configured to store identification information for more than one credit account, then an input for selecting between credit accounts is provided. The memory may be a flash memory. In an additional embodiment, the memory is integrated with the processor or the scanner so that the connections with the memory are not accessible for probing.

In an alternative embodiment, the credit card is integrated into a wrist watch.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a top view of a traditional credit card with a magnetic strip;

FIG. 2 is a top view of a credit card according to a first embodiment of the present invention;

FIG. 3 is a side view of a credit card according to a first embodiment of the present invention;

FIG. 4 is a top view of a credit card according to a second embodiment of the present invention;

FIG. 5 is a side view of a credit card according to a second embodiment of the present invention;

FIG. 6 is a top view of a credit card according to a third embodiment of the present invention;

FIG. 7 is a top view of a credit card according to a fourth embodiment of the present invention;

FIG. 8 is a perspective view of a wrist watch according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

A first embodiment of the present invention is shown in FIG. 2. As shown in FIG. 2, a credit card 10 is manufactured with a transmissive optical shutter 12. As shown in FIG. 3, the transmissive optical shutter allows light from a light source 14 to pass through the optical shutter 16 to a detector. As the light passes through the transmissive optical shutter 12, the optical shutter alters the light to convey information to the detector 16. In one embodiment of the present invention, the transmissive optical shutter 12 includes a liquid crystal display.

A second embodiment of the present invention is shown in FIG. 4. As shown in FIG. 4, a credit card 10 is manufactured with a retro-reflective optical shutter 20. As shown in FIG. 5, the retro-reflective optical shutter 20 reflects light from a light source 22 back toward a detector 24. When the light from the light source 22 is reflected to the detector 24, the light is altered by the optical shutter to convey information to the detector 24. In one embodiment of the present invention, the light is altered by a liquid crystal display. A card constructed in accordance with the second embodiment may be placed under a combination light source and detector system, thus providing convenience to the user.

A third embodiment of the present invention is shown in FIG. 6. As shown in FIG. 6, a credit card 10 is manufactured with an optical shutter 30, such as a transmissive optical shutter, or a retro-reflective optical shutter. In addition to the optical shutter, the credit card has a security system using fingerprint recognition. As explained below, data derived from a fingerprint of at least one particular finger of the card owner is stored in a non-erasable memory 32 located on the card.

At the time the card is used, the user places their fingers on the card so that at least a particular one of the user's

fingers is positioned over a scanner 34. A scan of the user's fingerprint is then made. A processor 36 compares data derived from a scan with data stored in the memory 32. If the fingerprint data stored in memory matches the data derived from the scan of the user's fingerprint, then a signal is sent to the optical shutter for transmission. If there is not a match, then no signal is sent to the optical shutter, and the card is unusable. In an additional embodiment, the card has function keys 38 for controlling functions of the card, such as beginning the scan of the user's finger. In another embodiment, the memory 32 of the card may store multiple account numbers and authorization codes, and the function keys 38 may be used to select among the different account numbers and authorization codes.

A fourth embodiment of the present invention is shown in FIG. 7. As shown in FIG. 7, a card is manufactured having an optical shutter 30 such as a transmissive optical shutter or a retro-reflective optical shutter. In addition to the optical shutter, the credit card has a security system using fingerprint recognition. An exemplary security system using fingerprint recognition is described above in reference to the third embodiment and includes a scanner, a non-volatile memory, and a processor. The non-volatile memory contains information including fingerprint information, an account number and security related codes. A card according to the fourth embodiment also has a solar cell which supplies power to the card. In an embodiment of the present invention, the memory of the card is written only once and cannot be reprogrammed or read.

The initialization of a card occurs, for example, as follows. A new card is given to the user and the initialization is completed inside of a bank or similar organization. An initializing machine is used to initialize the card. The initializing machine issues an account number for the user and

an optional security code. In an embodiment, the security code is a special number together with a checksum calculated by a special algorithm known only to the bank. The account number and the optional security code are transmitted from the initialization machine to the card through an input sensor, such as a photo sensor, on the card (Not shown).

If the card is equipped with a security system using fingerprint recognition, including a scanner, a non-volatile memory, and a processor, such as that described for the third and fourth embodiments described above, then the user holds the card so that the user's thumb is placed on the scanner of the card. The processing unit in the card takes an image signal of the fingerprint, goes through an algorithm, and converts the image signal into a set of numbers. The set of numbers which represents the fingerprint are then stored in the memory. In additional embodiments, for added security, the fingerprint can be transformed into numbers by several algorithms. The particular algorithm may be chosen during the initialization process and an identifier for the chosen algorithm stored in memory.

Once all of the necessary information has been placed in the memory, the card is ready for use. The card is programmed so that the input sensor cannot be used again, in order to prevent tampering with the stored information.

If the card is equipped with a security system using fingerprint recognition, including a scanner, a non-volatile memory, and a processor such as that described for the third and fourth embodiments described above, a transaction occurs as follows. During a transaction, a user holds the card so that the user's thumb is on the scanner. When the card is placed in proximity of the transaction machine, e.g. an ATM, the card will be powered up by a solar cell or battery if present, or through

electrical contacts on the surface of the card that interface with the transaction machine.

The processor reads the fingerprint and converts the fingerprint to a set of numbers based on the same algorithm used in initializing the card as determined by reference to an algorithm identifier stored on the card. If the set of numbers matches with the set of numbers stored in the memory that correspond to the user's fingerprint, then the card transmits a signal corresponding to the stored account number and the optional security code, if applicable, to the transaction machine. Thus, authenticity is checked and the user is allowed to continue with the transaction. If the fingerprint scan does not produce a set of numbers that match the set of numbers contained in the memory, then no action will be taken. Because the memory of the card cannot be read without the owner's fingerprint being correctly scanned, a lost card cannot be used by anyone. The advantage of using fingerprints this way is that the fingerprint information is retained in the card itself and is not transmitted anywhere else, thus making the user more comfortable in using it. Furthermore, if a flash memory is used, there is no way a user can reverse engineer the chip and find out the code, especially if the memory is integrated with the processing unit or the fingerprint scanner so that the interconnection of the memory circuit is inaccessible for probing.

For a more versatile card, the card can be programmed more generally so that two way communication may be established between a card and a transaction machine. This is desirable for smart card applications in which pertinent information is stored locally in the smart card itself rather than in the central database, as in the case of credit cards.

In an alternative embodiment of the present invention, initialization of a card equipped with a security system using

fingerprint recognition, proceeds as follows. The user is given a new card. The user holds the card so that the user's thumb is placed on the scanner of the card and places the card in an initialization machine. The processor in the card takes an image signal of the fingerprint, goes through an algorithm, and converts the image signal into a set of numbers. The set of numbers which represents the fingerprint is used as the bank account number.

The bank account number is communicated to the initialization machine by a transmitter on the card, such as an optical shutter. In another alternative embodiment, the set of numbers may be processed using an additional algorithm to arrive at a bank account number. The use of an additional algorithm prevents mischief by further preventing reconstruction of a user's identification information by others. By having the card transmit the account number to the bank, an input device, such as a photo-sensor is not necessary, and bank employees may be kept from a user's account information.

In yet another alternative embodiment, initialization of a card equipped with a security system using fingerprint recognition, proceeds as follows. A user is given a new card and allowed to take multiple fingerprint scans. The processor in the card takes each fingerprint image signal, goes through an algorithm, and converts the image signal into a set of numbers. The memory stores all of the sets of numbers from all of the individual scans. Later, when comparing a user's fingerprint, the processor compares the scan information to all of the sets of numbers stored in the memory. This lowers the rejection rate that a user encounters, and allows greater flexibility as to how the user places their finger on the scanner. In an additional embodiment, the user may scan multiple different fingers. In yet another embodiment, multiple users may scan their fingers on a single card, so that a family, for example, may all use the same

card. In an additional embodiment, each set of numbers formed by a scan is used as a bank account number so that one card is associated with multiple accounts which may or may not be linked together.

In another embodiment, the fingerprint authorization equipped credit card may be integrated with a time function and take the form of a wrist watch 60, as shown in FIG. 8. The watch 60 has a retro-reflective optical shutter 62 and a scanner 64. The retro-reflective optical shutter 62 also displays the time. Additionally, the watch 60 may have function keys 66 to complete traditional time-piece, credit card, and smart card functions.

Because the transaction is non-contact, there is no need for the user to take the watch off the wrist during the transaction. The user simply places their selected finger over the fingerprint sensor and place the watch under the active region of the transaction machine. The fingerprint will be read, checked against the memory, and the transaction will be initiated. For a smart card application where a two-way communication is needed, a photo sensor (not shown) can be added to the wrist watch for receiving data from the transaction machine. By integrating credit or smart card functionality with fingerprint authorization in a wrist watch, a user gains convenience, especially because the wrist watch is always ready to be used, and will not be lost easily.

In another embodiment, the fingerprint credit card can communicate with a transaction machine by using standard electrical contacts commonly used in smart cards. The use of standard electrical contacts commonly used in smart cards eliminates the added components of non-contact communication and power supply making it a simple card to use. The use of standard electrical contacts commonly used in smart cards also makes the card backward compatible with current systems. In yet another embodiment, the fingerprint credit card has a hybrid

communication scheme with the transaction machine in which both the electrical contacts and non-contact communication means are present at the same time, making the card compatible with both new and old transaction machines.

The preceding description has been presented with reference to the presently preferred embodiments of the invention shown in the drawings. Workers skilled in the art and technology to which this invention pertains will appreciate that alteration and changes in the described processes and structures can be practiced without departing from the spirit, principles and scope of this invention.

Accordingly, the present invention provides for a credit card with a fingerprint authorization system. Although this invention has been described in certain specific embodiments, many additional modifications and variations would be apparent to those skilled in the art. It is therefore to be understood that this invention may be practiced otherwise than as specifically described. Thus, the present embodiments of the invention should be considered in all respects as illustrative and not restrictive, the scope of the invention to be determined by the claims supported by this application and their equivalents rather than the foregoing description.

WHAT IS CLAIMED IS:

1. A credit card comprising:

a processor,

a memory, connected to the processor, storing credit card identification information for at least one credit account,

a scanner connected to the processor

a transmitter connected to the processor,

wherein the processor is programmed to a) receive reference fingerprint data from the scanner, b) store reference data based on the reference fingerprint data into the memory, c) receive test fingerprint data from the scanner at a time after the reference data is stored in memory, d) compare the reference data with test data based on the test fingerprint data and e) only if the comparison is within predefined limits, send the credit card identification information to the transmitter.

2. The credit card of claim 1, wherein the reference data is an identification code derived from the reference fingerprint data and wherein the test data is a test code derived from the test fingerprint data.

3. The credit card of claim 1, wherein the reference data is derived from the reference fingerprint data using a selected one of a plurality of algorithms, wherein an identification of the selected one of the plurality of algorithms is stored in the memory and wherein the test data is derived from the test fingerprint data based on the identification of the selected one of the plurality of algorithms.

4. The credit card of claim 1, wherein the reference data is a proper subset of the reference fingerprint data and the test data is a proper subset of the test fingerprint area.

5. The credit card of claim 1 wherein the memory only accepts the storing of the identification information once.

6. The credit card of claim 1 wherein the transmitter is one of the group of a transmissive shutter, a reflective shutter, an induction coil, an infrared transmitter, a radio transmitter and smart card electrical contacts.

7. The credit card of claim 1 further comprising a solar cell connected to the processor, memory and scanner.

8. The credit card of claim 1 wherein the memory stores credit card identification information for more than one credit account, the credit card further comprising an input for selecting between credit accounts.

9. The credit card of claim 1 further comprising a receiver.

10. The credit card of claim 9 wherein the receiver is one of the group consisting of an induction coil, an infrared receiver, a radio receiver and smart card electrical contacts.

11. The credit card of claim 1 wherein the memory is a flash memory.

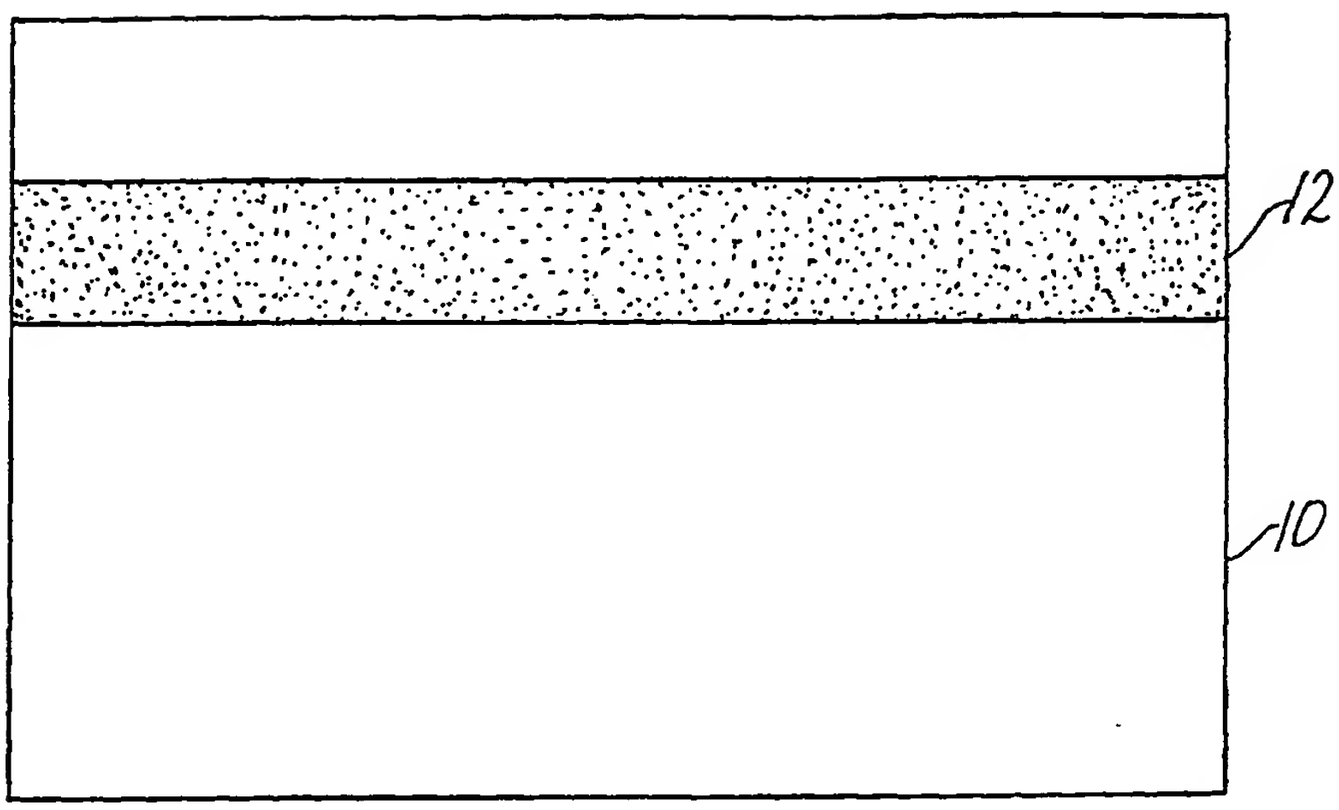
12. The credit card of claim 1 wherein the memory is integrated with the processor or the scanner such that the connections with the memory are not accessible for probing.

13. The credit card of claim 1 wherein the reference data is used as an account number and is transmitted by the transmitter to a bank to assign an account number to the card.

14. The credit card of claim 1 wherein the processor is programmed to receive reference fingerprint data from the scanner a plurality of times, each time storing additional reference data based on the reference fingerprint data into the memory; and wherein test data is compared to all of the reference data stored in memory.

15. The credit card of claim 1 wherein the credit card is integrated into a wrist watch.

Fig. 1



(PRIOR ART)

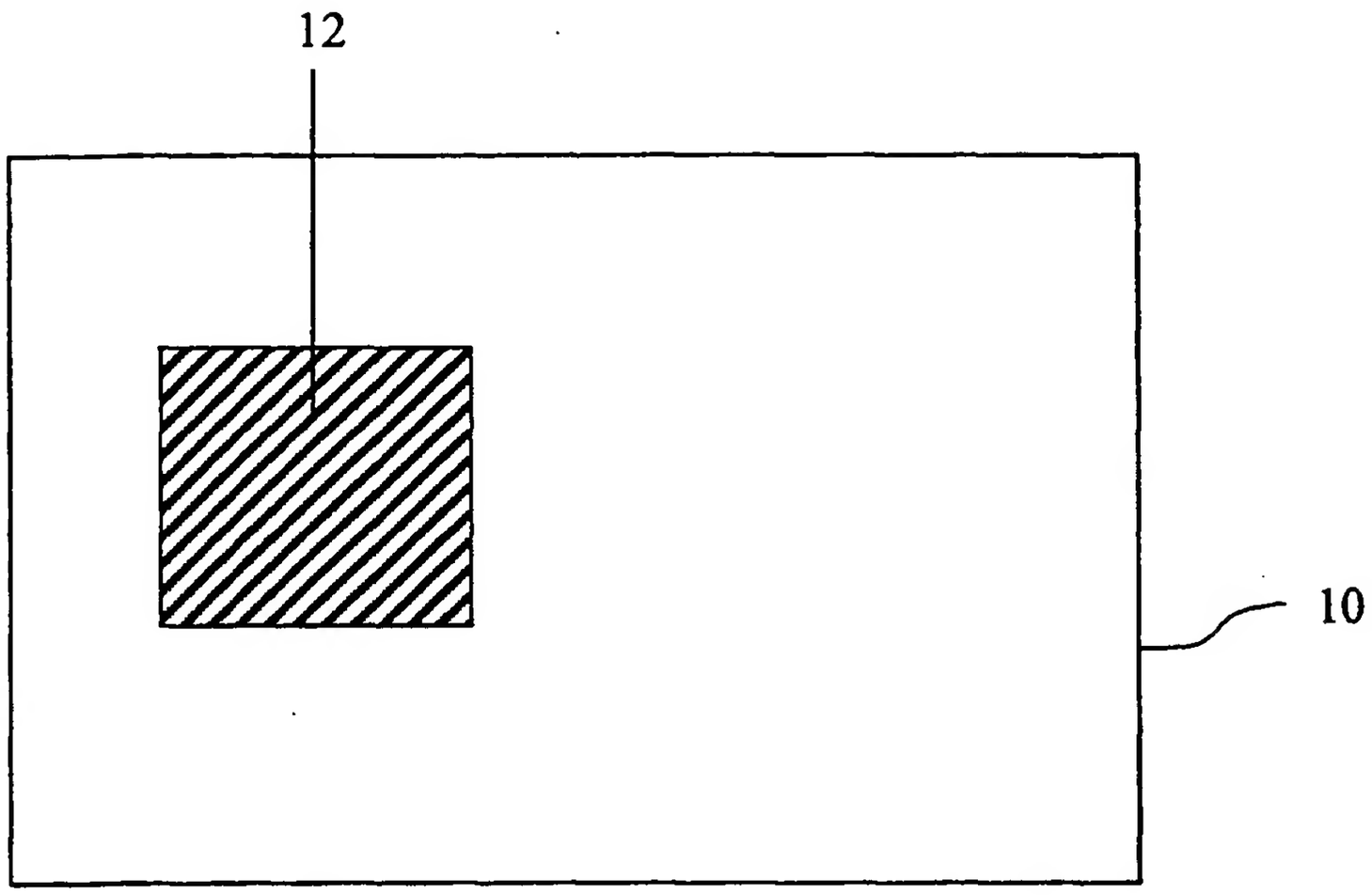


FIG. 2

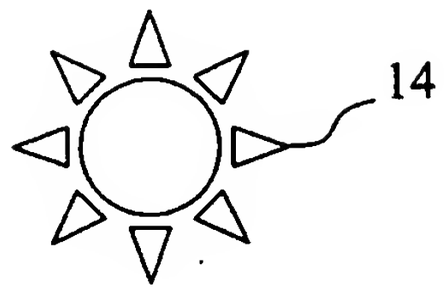


FIG. 3

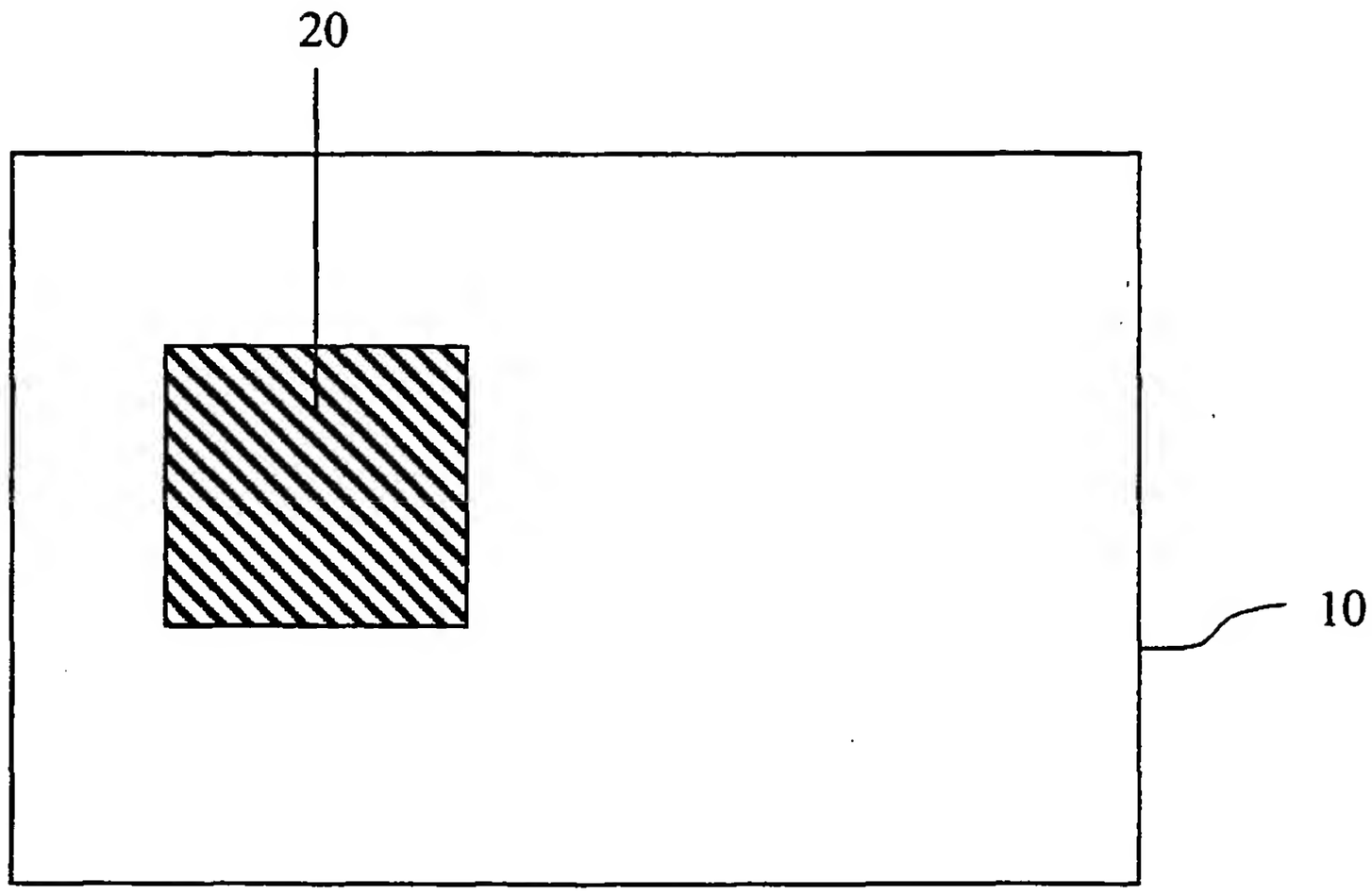
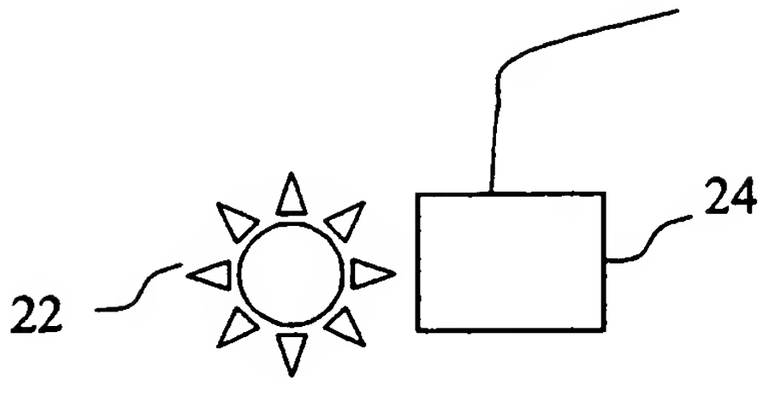


FIG. 4



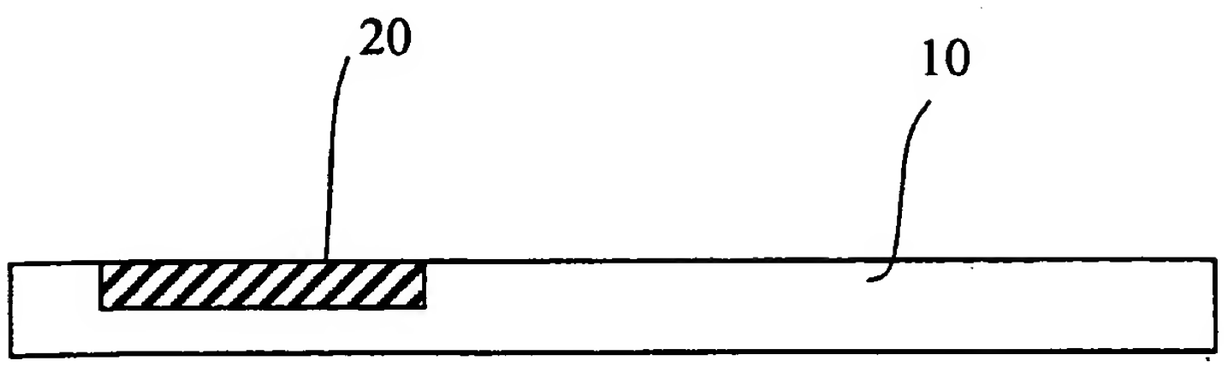


FIG. 5

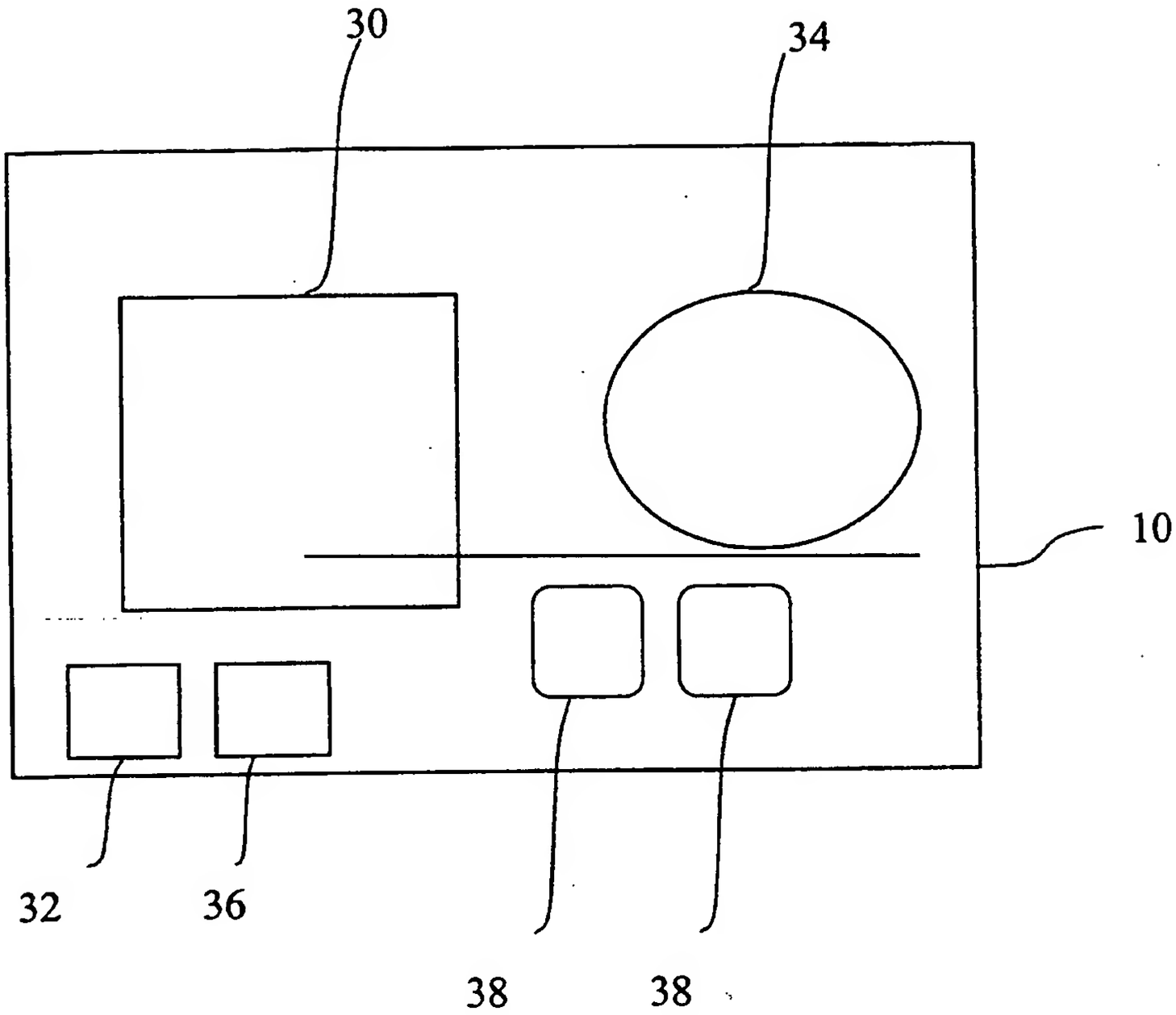


FIG. 6

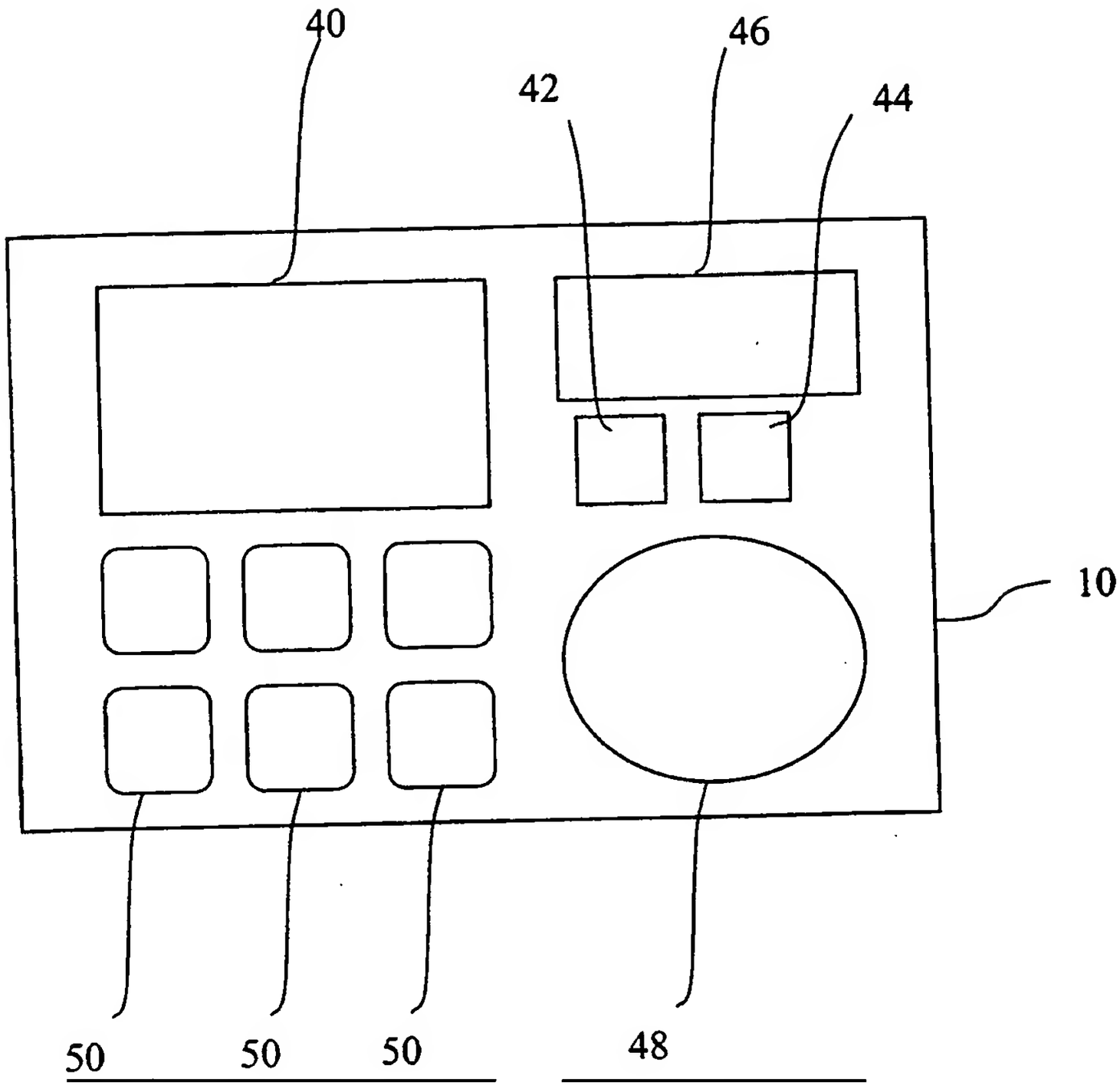
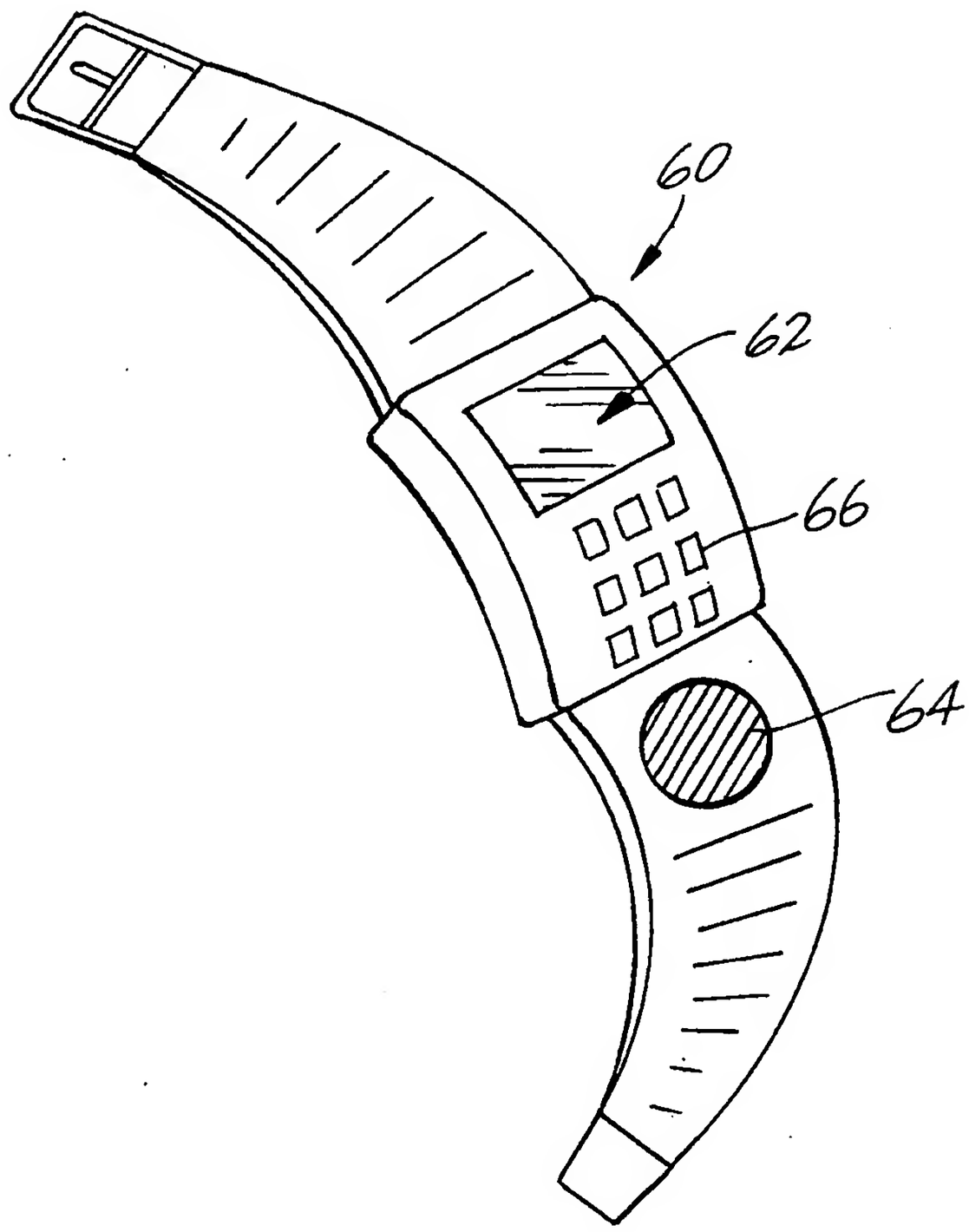


FIG. 7

Fig. 8



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/31425

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06K 19/06;G06K 5/00
US CL : 235/492, 380, 375, 379, 382

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 235/492, 380, 375, 379, 382; 902/3, 4, 5, 26

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
None

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,623,552 A (LANE et al) 22 April 1997 (22.04.1997), see entire document.	1-5
---		---
Y		6-7, 9-15
X	US 4,582,985 A (LOFBERG) 15 April 1986 (15.04.86), see entire document.	1-5
---		---
Y		7, 9-15
Y	US 4,746,787 A (SUTO et al) 24 May 1988 (24.5.88), see entire document.	6-7 and 12
Y	US 5,239,166 A (GRAVES) 24 August 1993 (24.08.93), see entire document.	8
Y	4,766,293 A (BOSTON) 23 August 1988 (23.08.88), see entire document.	8

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 January 2001 (29.01.2001)	02 MAR 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Diane I. Lee Telephone No. 703-306-3427

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US00/31425

Continuation of B. FIELDS SEARCHED Item 3: EAST database
search terms: (ic or credit or smart or chip or electronic) near3 card$2 same fingerprint$2 and (memory or storag) and (compar$4 same fingerprint) and ((receiv$4 or transmit$4 or antenna$2) same fingerprint same compar$4)